

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims of the application:

---

Claim 1 (Currently Amended) A method for mutual authentication of components in a network using the a challenge-response method ~~[[,]] in which, in order to~~ authenticate a terminal (M), ~~in particular a mobile station,~~ with the network, ~~the network (N) uses a request to request from an authentication center (AUC) comprising the steps of:~~ requesting at least one data pair comprising including a first random number (Challenge 1) and a first response (Response 1) [[,]] and passes from an authentication center using a request from the network;

a' passing the first random number (Challenge 1) to the terminal (M) which uses an internally stored key (K<sub>i</sub>) likewise and the first random number to calculate from this the first response (Response 1) and sends this ;

sending the calculated first response to the network (N), ~~in which case, furthermore, the network (N) is authenticated with the terminal (M) in that the terminal sends~~

sending a second random number (Challenge 2) from the terminal to the network [[,]] to which the network responds ; and

responding to the second random number with a second response (Response 2) calculated in the AUC authentication center, the response performed by the network, wherein

the first response (Response 1) sent from the terminal (M) to the network (N) is ~~at the same time~~ also used as the second random number (Challenge 2), ~~in which case~~ whereby the network has ~~already~~ previously requested the second response (Response 2) from the ~~AUC in advance~~, authentication center together with the first random number and the first response[[,]] as ~~part of~~ a triplet data set (Challenge 1/Response 1/Response 2).

Claim 2 (Currently Amended) The method as claimed in claim 1, wherein the network interprets the calculated first response (Response 1)[[,]] ~~which is~~ sent back from the terminal (M)[[,]] as the second random number (Challenge 2).

a' Claim 3 (Currently Amended) The method as claimed in claim 1 ~~or 2~~, wherein the first random number (Challenge 1) and the ~~first~~ second response (Response 2) are transmitted from the network (N) to the terminal (M) ~~immediately~~ successively in time succession.

Claim 4 (Currently Amended) The method as claimed in claim 1 ~~or 2~~, wherein ~~the~~ a data pair (Challenge 1/Response 2) is transmitted from the network (N) to the terminal (M) simultaneously[[,]] in the form of a single data set.

Claim 5 (Currently Amended) The method as claimed in ~~one of claims 2, 3 or 4~~ claim 1, wherein the network requests data sets from the authentication center ~~(AUC)~~ in the form of

triplet data sets (Challenge 1/Response 1/Response 2).

Claim 6 (Currently Amended) The method as claimed in claim 5, wherein a plurality of triplet data sets are supplied from the AUC authentication center as a stockpile[[,]] ~~in order to reduce the a~~ request frequency.

a' Claim 7 (Currently Amended) The method as claimed in claim ~~4 or 5~~ 1, wherein[[,]] ~~in order to use the first response (Response 1) of the terminal (M) as the second random number (Challenge 2) in order to authenticate the network with the terminal (M), the a~~ shorter length of the first response (Response 1) is filled out to make up ~~the a~~ greater length of the second random number (Challenge 2).

Claim 8 (Currently Amended) The method as claimed in claim 7, wherein

the filling-out ~~process is carried out~~ performed on a subscriber-specific basis[[,]] ; and ~~wherein~~

the complete length of the first response (Response 1) is shortened before transmission to ~~the an~~ other station.

Claim 9 (Currently Amended) The method as claimed in claim 8, wherein the first response (Response 1) is filled out with defined bits from the ~~secret~~ key (Ki) to make up the length of the second random number (Challenge 2).

Claim 10 (Currently Amended) The method as claimed in

claim 8, wherein the second random number (Challenge) corresponds to the ~~original~~ first response (Response 1) before it was shortened.

Claim 11 (Currently Amended) The method as claimed in ~~one of claims 1-10~~ claim 1, wherein the network is a GSM network.

Claim 12 (Currently Amended) The method as claimed in ~~one of claims 1-10~~ claim 1, wherein the network is a wire-based network.

a  
Claim 13 (Currently Amended) The method as claimed in claim 12, wherein ~~the individual, mutually authenticating~~ components in ~~[[a]]~~ the wire-based network are different monitoring units of computers which authenticate themselves with a central computer, and vice versa.

Claim 14 (Currently Amended) The method as claimed in ~~one of claims 1-13~~ claim 1, wherein the AUC authentication center calculates the triplet data sets requested by the network and transmits ~~these~~ the calculated triplet data sets to the network off-line and independently of time, on request by the network, ~~but in any case~~ and before ~~the~~ data interchange between the network and the terminal.

---